

IN THE CLAIMS

Following are the current claims. For the claims that have **NOT** been amended in this response, any difference between the claims below and the current state of the claims is unintentional and in the nature of a typographical error:

1. (Currently Amended) A method of enhancing throughput of a multi-stage pipelined encryption/decryption engine for an encryption/decryption process when used with an encryption/decryption mode of operation requiring feedback around the pipelined engine, the method comprising the steps of:

aggregating together multiple security contexts and establishing an entry in a bank of initial variables for each context, there being at least as many encryption/decryption security context identifiers as a predetermined number of stages in the encryption/decryption process;

receiving, for input to the multi-stage pipelined encryption/decryption engine, a source datablock for a given encryption/decryption security context identifier;

indexing according to the encryption/decryption security context identifier into the bank of initial variables to retrieve an initial variable for the source datablock, the bank comprising a plurality of initial variables for each encryption/decryption security context identifier;

generating an output datablock from the source datablock and its corresponding initial variable; and

replacing [an] the initial variable in the bank of initial variables with a new seed, as determined by a selected mode of operation, for the security context identifier.

2. (Canceled)

3. (Canceled)

4. (Previously Amended) The method of claim 1 wherein the mode of operation of the encryption/decryption process requires feedback around the encryption/decryption engine such as Cipher Block Chaining Mode with exception of handling of initial variables.

5. (Currently Amended) The method of claim [4] 1 wherein the encryption/decryption process comprises a block cipher capable of being pipelined such as Digital Encryption Standard (DES).

6. (Canceled)

7. (Canceled)

8. (Canceled)

9. (Canceled)

10. (Canceled)

11. (Canceled)

12. (Currently Amended) A multi-stage pipelined encryption engine for an encryption/decryption process when used with an encryption/decryption mode of operation requiring feedback around the stages, the encryption/decryption engine comprising:

means for aggregating together multiple security contexts and establishing an entry in a bank of initial variables for each context, there being at least as many encryption/decryption security context identifiers as a predetermined number of stages in the encryption/decryption process;

means for receiving, for input to the multi-stage pipelined encryption/decryption engine, a source datablock for a given encryption/decryption security context identifier, there being at least as many encryption/decryption security context identifiers as the predetermined number of stages in the encryption/decryption process;

means for indexing according to the encryption/decryption security context identifier into a bank of initial variables to retrieve an initial variable for the source datablock, the bank comprising a plurality of initial variables for each encryption/decryption security context identifier;

means for generating an output datablock from the source datablock and its corresponding initial variable; and

means for replacing [an] the initial variable in the bank of initial variables with a new seed, as determined by a selected mode of operation, for the security context identifier.

13. (Canceled)

14. (Canceled)

15. (Previously Amended) The encryption/decryption engine of claim 12 wherein the mode of operation of the encryption/decryption process requires feedback around the encryption/decryption engine such as Cipher Block Chaining Mode with exception of handling of initial variables.

16. (Currently Amended) The encryption/decryption engine of claim [15] 12 wherein the encryption/decryption process comprises a block cipher capable of being pipelined such as Digital Encryption Standard (DES).

17. (Canceled)

18. (Canceled)

19. (Canceled)

20. (Canceled)

21. (Canceled)

22. (Currently Amended) A method of enhancing throughput of a multi-stage pipelined encryption/decryption engine for an encryption/decryption process when used with an encryption/decryption mode of operation requiring feedback around the pipelined engine, the method comprising the steps of:

separating one data stream into multiple interleaved data streams, each having its own encryption/decryption security context;

aggregating together the multiple security contexts and establishing an entry in a bank of initial variables for each context, there being at least as many encryption/decryption security context identifiers as a predetermined number of stages in the encryption/decryption process;

receiving, for input to the multi-stage pipelined encryption/decryption engine, a source datablock for a given encryption/decryption security context identifier[, there being at least as many encryption/decryption security context identifiers as the predetermined number of stages in the encryption/decryption process];

indexing according to the encryption/decryption security context identifier into the bank of initial variables to retrieve an initial variable for the source datablock, the bank comprising a plurality of initial variables for each encryption/decryption security context identifier;

generating an output datablock from the source datablock and its corresponding initial variable; and

replacing [an] the initial variable in the bank of initial variables with a new seed, as determined by a selected mode of operation, for the security context identifier.

23. (Previously Added) The method of claim 22 wherein the mode of operation of the encryption/decryption process requires feedback around the encryption/decryption engine such as Cipher Block Chaining Mode with exception of handling of initial variables.

24. (Currently Amended) The method of claim [23] 22 wherein the encryption/decryption process comprises a block cipher capable of being pipelined such as Digital Encryption Standard (DES).

25. (Currently Amended) A multi-stage pipelined encryption engine for an encryption/decryption process when used with an encryption/decryption mode of operation requiring feedback around the stages, the encryption/decryption engine comprising:

means for separating one data stream into multiple interleaved data streams, each having its own encryption/decryption security context

means for aggregating together the multiple security contexts and establishing an entry in a bank of initial variables for each context, there being at least as many encryption/decryption security context identifiers as a predetermined number of stages in the encryption/decryption process;

means for receiving, for input to the multi-stage pipelined encryption/decryption engine, a source datablock for a given encryption/decryption security context identifier, there being at least as many encryption/decryption security context identifiers as the predetermined number of stages in the encryption/decryption process;

means for indexing according to the encryption/decryption security context identifier into a bank of initial variables to retrieve an initial variable for the source datablock, the bank comprising a plurality of initial variables for each encryption/decryption security context identifier;

means for generating an output datablock from the source datablock and its corresponding initial variable; and

means for replacing [an] the initial variable in the bank of initial variables with a new seed, as determined by a selected mode of operation, for the security context identifier.

26. (Currently Amended) The encryption/decryption engine of claim 25 wherein the mode of operation of the encryption/decryption process requires feedback around the encryption/decryption engine such as Cipher Block Chaining Mode with exception of handling of initial variables.

27. (Currently Amended) The encryption/decryption engine of claim [26] 25 wherein the encryption/decryption process comprises a block cipher capable of being pipelined such as Digital Encryption Standard (DES).